Information Techonolgy Contractual Requirements for Software as a Service (SaaS) Solutions

Req. ID	Category	Subcategory	Requirement Description	Response	Explantion
IT1	Security	Standard Policy	The State of Alaska (and by extension DOH) requires that all business and technical resources utilized under the contract, including system development, testing, implementation, training, and hosting be**United States based**. This includes hosted services, vendor personnel, vendor contracted services, contracted consulting services, and any sub-contracted resources. All elements and services that receive, process, store, or transmit data used by the solution must be hosted within the United States.		
IT2	Investment Assurance	Asset Management	DOH shall have unlimited rights to use, disclose or duplicate, for any purpose whatsoever, all information and data developed, derived, documented, installed, improved, or furnished by the offeror under this contract. All files containing any DOH information are the sole and exclusive property of DOH. The offeror agrees not to use information obtained for any purposes not directly related to this contract without prior written permission from DOH. Offeror agrees to abide by all federal and state confidentiality requirements.		
IT3	Investment Assurance	Asset Management	The offeror agrees to provide to DOH, upon request at any time during the contracted period, the data managed by the solution, in whole or in part, in a format agreed upon by both parties.		
IT4	Integration	Data Exchange	The offeror agrees to align their solution with DOH's System Integration Services and standards. Data exchanges between this solution, and other DOH data, will be conducted through DOH's Enterprise Service Bus.		
IT5	Integration	Data Exchange	Solutions that create, read, or update client, consumer, or other person demographic data must integrate with DOH's Master Client Index (MCI) to ensure their demographic records are registered in the MCI and appropriately merged with matching client records in the index.		
IT6	Integration	Authentication	The offeror must integrate their solution with the Alaska DOH's Active Directory or DOH's Active Directory Federated Services (ADFS) to support single sign-on authentication.		
IT7	Integration	Financial and Accounting	Offerors whose proposed solution includes finance, accounting, and Human Resources (HR) functions agree to conduct a gap analysis with DOH ITS, DOH Program staff, and Department of Administration Division of Finance Integrated Resource Information System (IRIS) support subject matter experts. This analysis will determine how the solution will integrate with the State of Alaska's existing Human Resources and Finance/Accounting systems.		
IT8	Security	Code Security	The offeror must complete software development in compliance with DOH Secure Systems Development Lifecycle, including: • Secure Coding – The offeror shall disclose what tools are used in the software development environment to encourage secure coding. • Disclosure – The offeror shall document in writing to the purchaser all third-party software used in the software, including all libraries, frameworks, components, and other products, whether commercial, free, open-source, or proprietary. • Evaluation – The offeror shall make reasonable efforts to ensure third-party software meets all the terms of this agreement and is as secure as the custom code developed under this agreement. • Source Code Scanning – The offeror shall work with DOH staff to facilitate static code scanning for all product and third-party files using a DOH provided scanning solution. • Hosting Environment Hardening – The offeror shall work with DOH staff to ensure that any hosting environment utilized complies with DOH's adopted standards for security hardening.		

IT9	Security	Code Security	The offeror shall document in writing to the Purchaser all third-party software used in the software, including all libraries, frameworks, components, and other products, whether commercial, free, open-source, or proprietary.		
IT10	Security	Environment	The offeror shall work with DOH staff to ensure that any hosting environment utilized complies with DOH adopted standards for security hardening. The offeror acknowledges that all DOH Information Security Compliance and Privacy Services and Standards apply to DOH managed off-site hosting scenarios.		
IT11	Security	Environment	Offeror shall facilitate requests for third-party vulnerability and/or penetration testing of DOH solutions.		
IT12	Security	Policy	The offeror agrees to notify, in writing, the DOH contract administrator of any personnel transfers or termination of their personnel, including sub-contractors, who possess DOH credentials and/or badges or who have DOH information system previledges, within fifteen (15) calendar days.		
IT13	Security	Retention/Destruction	The offeror agrees to dispose of all protected printed media in a manner consistent with the guidance provided by the National Instiitute of Technologies (NIST) Special Publication 800-88 Revision 1. This includes any Development, Test, and Production data.		
IT14	Security	Retention/Destruction	The offeror must ensure that all protected electronic media (electronic protected health information [PHI], personally identifiable information [PII], protected information [PI], protected client information [PCI], criminal justice information [CJI], etc.) must be disposed of in a manner consistent with the guidance provided by the Department of the Army's brief, Cybersecurity: Sanitization of Media and NIST Special Publication 800-88 Revision 1. Disposed of electronic media must receive a Certificate of Media Disposal or agreed upon proof of disposal for each device disposed.		
IT15	Security	Retention/Destruction	The offeror ensures that the solution will comply with DOH's policies for record retention. The offeror must provide procedures and agree to all data (including test data) destruction when contract ends if continuing operations and maintenance is not provided by the contractor. The offeror must provide an information system with an audit reduction and report generation capability that: a. Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents; b. Does not alter the original content or time ordering of audit records; c. Retains audit records for at least ninety (90) days and archives old records for six (6) years to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements		
IT16	Security	Authorization Package	Solutions must be granted Authority to Operate before they can be used to support DOH activities. Actual workload varies greatly in proportion to the size of the solution and offeror's experience demonstrating security compliance. We have found that most small to medium size solutions require 80–120 hours to complete the initial security control responses. The offeror agrees to work towards security compliance requirements and accommodate an appropriate number of remediation cycles to address any identified defects.		
IT17	Security	Authorization Package	The offeror agrees to submit one Interface Risk Assessment Worksheet, per interface, outliing its specifications and security components		
IT18	Security	Encryption	The offeror confirms their solution ensures all sensitive, confidential, and/or restricted data are encrypted in-transit and at-rest. Criminal Justice Information Systems (CJIS) and those systems requiring Minimum Acceptable Risk Safeguards for Exchanges (MARS-E) compliance must meet these encryption requirements using a Federal Information Processing Standards (FIPS) 140-2 certified product.		

IT19	Desktop/Device	Standards	Offeror confirms their solution is device independent and/or fully functional operating on a Microsoft Windows desktop/laptop with standard Microsoft productivity suite software. Offeror's proposed solutions must operate on standard OIT-specified equipment (subject to annual review) Any solution specific requirements such as drivers, software versions, etc. should be described in Comments.		
IT20	Desktop/Device	Standards	Offeror confirms their solution does not require elevated permissions for the end-user on their device.		
IT21	Mobile Device	Standards	If solution includes mobile devices, offeror confirms their solution will be fully functional with the standard DOH mobile devices: • Dell Windows based Tablets o Configured with the latest version of Microsoft Standard browsers o Web applications are to be Browser version independent which means they support current versions of Internet browsers for Microsoft, FireFox, and Google Chrome. o Software should not be dependent on a specific version of MS Office Suite. • Apple iOS based Tablets and Smart Phones o Configured with the latest version of Safari and Google Chrome. o Software should not be dependent on a specific version of MS Office Suite The offeror confirms their solution: a. Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices; b. Authorizes the connection of mobile devices to organizational information systems. c. Establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to access the information system from external information systems; and process, store, or transmit organization-controlled information using external information systems.		
IT22	WAN	General	Bandwidth varies greatly in areas outside Juneau, Anchorage, Wasilla, and Fairbanks. In some rural communities bandwidth can be as low as 56k. The Offeror agrees to denote any performance degredation that could be encountered by their solution along with suggested mitigations.		
IT23	Accessibilty	Standards	The offeror attests their solution is compliant with accessibility standards and assistive/adaptable technology accommodations for users with disabilities under the latest or most current Federal and State regulations, including but not limited to: a. ADA (section508.gov) b. W3C (w3.org). Accessibility issues are categorized in four distinct groups under Web Content Accessibility Guidelines (WCAG). • Perceivable issues are those that affect a user's ability to find and process information on a website • Operable issues are those that impact a visitor's ability to navigate and use a website • Understandable issues concern a user's ability to discern and comprehend all information and navigation on a website • Robust issues involve a website's ability to adapt and evolve to meet the changing needs of users with disabilities ADA areas of concern include: • Structure • Readability • Descriptive Link Text • Accessible Files • Videos • Images • Color • Fonts • Keyboard Navigation • Form and Table Labels • Call-to-Action (CTA) Buttons		
IT24	Architecture and Performance	Architecture	The offeror attests their solution was developed using modern design principles, applying principles of modularity, interface abstraction, and loose coupling to support ease of maintenance and readily allow future functional enhancements.		
IT25	Architecture and Performance	Architecture	The offeror ensures that functionality added for other customers will not negatively impact DOH's solution instance.		

<table>
<tr><td>IT26</td><td>Hosting and Support</td><td>Standards</td><td>The offeror will work with DOH to determine content and schedule of system upgrades.</td><td></td><td></td></tr>
<tr><td>IT27</td><td>Security</td><td>Architecture</td><td>The offeror attests their solution will be hosted in a federally-compliant cloud-based or hybrid-cloud based hosting model (public, private, or government cloud).</td><td></td><td></td></tr>
<tr><td>IT28</td><td>Investment Assurance</td><td>Standards</td><td>The offeror's solution will offer continuous backup with geographically separated redundancy.</td><td></td><td></td></tr>
<tr><td>IT29</td><td>Security</td><td>Auditing and Logging</td><td>The offeror ensures their solution maintains an audit log as outlined below.

The offeror's solution will log the following events, per record:
a. Record was created/modified
b. Record was deleted
c. Record was viewed
d. Record was printed
e. Record was searched
f. System login (both successful and unsuccessful)
g. System logout

Their log entries will include, at minimum:
a. The user ID of the person who accessed the record
b. The date and time of the event
c. Network location
d. The information that was accessed
e. The record's data state before and after any edits

These Audit records will be maintained for investigative purposes and should be readily searchable by user ID or client ID.

In addition, for solutions hosted by DOH, the offeror confirms their solution can submit logged events to DOH's industry standard Security Information and Event Management (SIEM) solution.

The offeror must provide an information system with an audit reduction and report generation capability that:
a. Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents;
b. Does not alter the original content or time ordering of audit records;
c. Retains audit records for at least ninety (90) days and archives old records for six (6) years to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.</td><td></td><td></td></tr>
<tr><td>IT30</td><td>Availability</td><td></td><td>The offeror attests to the level of availability that they will deliver.

The highest availability standard for systems is 99.999% or “five nines”–or about 5 minutes and 15 seconds of downtime per year (see table below). To achieve five nines, all components of the system must work seamlessly together. Software applications, compute resources, networking functionality, and physical data center services must be highly available to achieve five nines.

<table>
<tr><th>Availability</th><th>Downtime / Year</th><th>Downtime / Month</th><th>Downtime / Week</th><th>Downtime / Day</th></tr>
<tr><td>99.999%</td><td>5.256 Minutes</td><td>0.438 Minutes</td><td>0.101 Minutes</td><td>0.014 Minutes</td></tr>
<tr><td>99.995%</td><td>26.28 Minutes</td><td>2.19 Minutes</td><td>0.505 Minutes</td><td>0.072 Minutes</td></tr>
<tr><td>99.990%</td><td>52.56 Minutes</td><td>4.38 Minutes</td><td>1.011 Minutes</td><td>0.144 Minutes</td></tr>
<tr><td>99.950%</td><td>4.38 Hours</td><td>21.9 Minutes</td><td>5.054 Minutes</td><td>0.72 Minutes</td></tr>
<tr><td>99.900%</td><td>8.76 Hours</td><td>43.8 Minutes</td><td>10.108 Minutes</td><td>1.44 Minutes</td></tr>
<tr><td>99.500%</td><td>43.8 Hours</td><td>3.65 Hours</td><td>50.538 Minutes</td><td>7.2 Minutes</td></tr>
<tr><td>99.250%</td><td>65.7 Hours</td><td>5.475 Hours</td><td>75.808 Minutes</td><td>10.8 Minutes</td></tr>
<tr><td>99.000%</td><td>87.6 Hours</td><td>7.3 Hours</td><td>101.077 Minutes</td><td>14.4 Minutes</td></tr>
</table></td><td></td><td></td></tr>
</table>

IT31	Database		The offeror attests they maintain database design and maintenance best practices, including provisions for: • Deploying Firewalls for Database Servers • Ensuring database software is patched to include all current security patches • Maintaining application code that is reviewed for SQL injection vulnerabilities • Monitoring the delivery of protected data to user workstations • Passwords for all database administrator (DBA), operating system accounts, and database accounts are required to be strong passwords • Secure authentication to the database is used • Tracking all logins to operating system and database servers, successful or unsuccessful • Protected data is encrypted at rest, as well as during transmission over the network		
IT32	Reporting		The Offeror attests that any reporting capability contained within the solution will employ Embedded Data Analytics, features including: • Application Programming Interface (API) Integration • Extract, Transform, and Load (ETL) integration • Data Variety Support • Data Modeling Capability • Data Quality Monitoring and Remediation • Real-Time Performance Optimization • Scalability • Robust Security Controls • Data Privacy and Governance Controls		
IT33	Security		The offeror must acknowledge, and commit to implementing the following application security standards: • Open Web Application Security Project (OWASP) Protocols • NIST Special Publication (SP) 800–218 Guidelines • International Organization for Standardization (ISO) 27034 Measures • Center for Internet Security (CIS) Control 16: Application Software Security Controls • Payment Card Industry (PCI) Payment Application Data Security Standard (PA-DSS) (whenever any payment controls are included in an application)		
IT34	Mobile Device		The Offeror acknowledges that if their solution includes a mobile app companion to any system, or a purely mobile solution, they ensure their solution: • Integrates Push Notifications into App Functions • Provides High-Quality Image Resolution • Includes an Integrated Search Feature • Incorporates Social Media Integration Capability • Uses Responsive App Design • Follows the Principle of Simplicity-in-Design, with Uncluttered Elements (https://www.cerdonis.tech/blogs/the-process-of-mobile-app-designing/) • Complies with General Data Protection Regulations (GDPR) Standards • Incorporates Machine Learning Attributes • Allows for the Integration of Augmented Reality • Provides Extensive Cross-Platform Coverage and usability • Incorporates Robust Security Controls • Leverages Mobile Screen Touch Features • Integrates Provisions for User Feedback • Provides the Ability for Apps to Work Offline		

Offeror's Name:

The purpose of the cost proposal format below is to allow Offerors to submit pricing in a consistent manner that the State can evaluate and score. The State has provided the desired rate type multipliers to provide a mechanism to correlate costs to the anticipated budget. These estimates are not a guarantee of services or payment, which will be paid via the contract, for actual services provided.

Proposals will be evaluated on Section 1 below. Total project cost in excess of $20,000,000.00 will cause the proposal to be considered non-responsive and be rejected.

Please enter your costs in the spaces provided below for each role, material, and any additional costs that will be incurred. All costs proposed in each section below must include all anticipated expenses, including scheduling, communication, implementation, and documentation. No additional costs may be billed to the contract without prior approval by the State, via a contract amendment.

Section 1 **This section will be included in the evaluation scoring process.**			
Role (please provide a separate line for every role required) Note: at a minimum key staff positions must be named in this table	**Hourly rate for the contract period**	**Estimated hours for the contract period**	**Estimated cost for the contract period**
Sample Project Manager	$ 75.00	15000	$ 1,125,000.00
Sample Scrum Master	$ 75.00	11000	$ 825,000.00
Sample Technical Lead	$ 175.00	18000	$ 3,150,000.00
Sample Developers	$ 100.00	45000	$ 4,500,000.00
Sample ECM Professional	$ 100.00	15000	$ 1,500,000.00
Sample Researcher	$ 75.00	15000	$ 1,125,000.00
Sample User Experience/Visual Designer	$ 75.00	15000	$ 1,125,000.00
Sample Business Analyst	$ 75.00	15000	$ 1,125,000.00
Sample Eligibility & Enrollment Subject Matter Expert (SME)	$ 100.00	15000	$ 1,500,000.00
Sample Security Consultant	$ 150.00	15000	$ 2,250,000.00
Sample Quality Assurance	$ 100.00	15000	$ 1,500,000.00
***Note: delete above and add your roles, rates, and hours.			$ -
The items above are for illustration purposes***			$ -
			$ -
			$ -
			$ -
			$ -
			$ -
			$ -
		Section 1 Total	**$ 19,725,000.00**

Section 2 **The below costs will not be used to directly compare offeror's proposals for the purposes of the evaluation scoring process but will be considered for the resulting contract. The total costs for staffing above and the costs below must not exceed the total project budget of $20,000,000.00.**	
Materials, travel, and all other non-personnel project costs (please itemize categories)	**Estimated cost for the contract period**
Sample Travel	$ 10,000.00
Sample Supplies	$ 2,000.00
***Note: delete above and add your roles, rates, and hours. The items above are for	
illustration purposes***	
Section 2 Total	**$ 12,000.00**
TOTAL PROJECT BUDGET (not to exceed $20,000,000.00)	**$ 19,737,000.00**